Cyber–Physical System Security of Distribution Systems

Other titles in Foundations and Trends® in Electric Energy Systems

Network-Based Analysis of Rotor Angle Stability of Power Systems
Yue Song, David J. Hill and Tao Liu
ISBN: 978-1-68083-778-0

A Survey of Relaxations and Approximations of the Power Flow Equations
Daniel K. Molzahn and Ian A. Hiskens
ISBN: 978-1-68083-540-3

HELM: The Holomorphic Embedding Load-Flow Method. Foundations and Implementations
Antonio Trias
ISBN: 978-1-68083-516-8

Combinatorial Optimization of Alternating Current Electric Power Systems
Sid Chi-Kin Chau
ISBN: 978-1-68083-514-4

Cyber–Physical System Security of Distribution Systems

Chen-Ching Liu
Virginia Tech

Juan C. Bedoya
Virginia Tech

Nitasha Sahani
Virginia Tech

Alexandru Stefanov
Delft University of Technology

Jennifer Appiah-Kubi
Virginia Tech

Chih-Che Sun
Washington State University

Jin Young Lee
Washington State University

Ruoxi Zhu
Virginia Tech

now
the essence of knowledge
Boston — Delft

Foundations and Trends® in Electric Energy Systems

Published, sold and distributed by:
now Publishers Inc.
PO Box 1024
Hanover, MA 02339
United States
Tel. +1-781-985-4510
www.nowpublishers.com
sales@nowpublishers.com

Outside North America:
now Publishers Inc.
PO Box 179
2600 AD Delft
The Netherlands
Tel. +31-6-51115274

The preferred citation for this publication is

C.-C. Liu, J. C. Bedoya, N. Sahani, A. Stefanov, J. Appiah-Kubi, C.-C. Sun, J. Y. Lee and R. Zhu. *Cyber–Physical System Security of Distribution Systems*. Foundations and Trends® in Electric Energy Systems, vol. 4, no. 4, pp. 346–410, 2021.

ISBN: 978-1-68083-853-4

Foundations and Trends® in Electric Energy Systems

Volume 4, Issue 4, 2021

Editorial Board

Editorial Scope

Topics

Foundations and Trends® in Electric Energy Systems publishes survey and tutorial articles in the following topics:

- Advances in power dispatch
- Demand-side and grid scale data analytics
- Design and optimization of electric services
- Distributed control and optimization of distribution networks
- Distributed sensing for the grid
- Distribution systems
- Fault location and service restoration
- Integration of physics-based and data-driven modeling of future electric energy systems
- Integration of Power electronics, Networked FACTS
- Integration of renewable energy sources
- Interdependence of power system operations and planning and the electricity markets
- Microgrids
- Modern grid architecture
- Power system analysis and computing
- Power system dynamics
- Power system operation
- Power system planning
- Power system reliability
- Power system transients
- Security and privacy
- Stability and control for the whole multi-layer (granulated) network with new load models (to include storage, DR, EVs) and new generation
- System protection and control
- The new stability guidelines and control structures for supporting high penetration of renewables (>50%)
- Uncertainty quantification for the grid
- System impacts of HVDC

Information for Librarians

Foundations and Trends® in Electric Energy Systems, 2021, Volume 4, 4 issues. ISSN paper version 2332-6557. ISSN online version 2332-6565. Also available as a combined paper and online subscription.

Contents

Cyber–Physical System Security of Distribution Systems

Chen-Ching Liu[1], Juan C. Bedoya[1], Nitasha Sahani[1], Alexandru Stefanov[2], Jennifer Appiah-Kubi[1], Chih-Che Sun[3], Jin Young Lee[3] and Ruoxi Zhu[1]

[1] *Virginia Tech, USA; ccliu@vt.edu*
[2] *Delft University of Technology, Netherlands*
[3] *Washington State University, USA*

ABSTRACT

The Information and Communications Technology (ICT) for control and monitoring of power systems is a layer on top of the physical power system infrastructure. The cyber system and physical power system components form a tightly coupled Cyber–Physical System (CPS). Sources of vulnerabilities arise from the computing and communication systems of the cyber–power grid. Cyber intrusions targeting the power grid are serious threats to the reliability of electricity supply that is critical to society and the economy. In a typical Information Technology environment, numerous attack scenarios have shown how unauthorized users can access and manipulate protected information from a network domain. The need for cyber security has led to industry standards that power grids must meet to ensure that the monitoring, operation, and control functions are not disrupted by cyber intrusions. Cyber security technologies such as encryption and authentication have been deployed on the CPS. Intrusion or anomaly detection and mitigation

Chen-Ching Liu, Juan C. Bedoya, Nitasha Sahani, Alexandru Stefanov, Jennifer Appiah-Kubi, Chih-Che Sun, Jin Young Lee and Ruoxi Zhu (2021), "Cyber–Physical System Security of Distribution Systems", Foundations and Trends® in Electric Energy Systems: Vol. 4, No. 4, pp 346–410. DOI: 10.1561/3100000026.

tools developed for power grids are emerging. This survey paper provides the basic concepts of cyber vulnerabilities of distribution systems and CPS security. The important ICT subjects for distribution systems covered in this paper include Supervisory Control And Data Acquisition, Distributed Energy Resources, including renewable energy and smart meters.

1

Introduction

Threats of cyberattacks targeting the electric power grid have been increasing in recent years (SANS, 2016; Clavel *et al.*, 2015). The consequence of cyber incidents on the power grid includes equipment damage, cascading events, large-scale power outages, and disruption of market functions (Cheng *et al.*, 2017; Sridhar *et al.*, 2012; Spolar, 2012). Government and industry have made a significant effort to strengthen the protection of the power infrastructure against cyber threats by setting standards and guidelines (e.g., Smith, 2014; Khalifa *et al.*, 2011; Sun *et al.*, 2016; Sun *et al.*, 2018; NIST, 2010; NIST, 2014).

- Critical Infrastructure Protection, Presidential Directive PDD-63, 1998.
- Cyber Security Roadmap for Energy Delivery Systems, Department of Energy (DOE), 2011.
- Guidelines for Smart Grid Cyber Security, National Institute of Standards and Technology (NIST) Report 7628.
- Critical Infrastructure Protection (CIP) Standards, Cyber Security CIP 002-014, North American Electric Reliability Corporation (NERC).

- National Electric Sector Cybersecurity Organization Resource (NESCOR), Electric Power Research Institute (EPRI).
- European Programme for Critical Infrastructure Protection (EPCIP) resulting from the European Commission's directive EU COM (2006).

As power systems become more complex and dependent on the Information and Communications Technology (ICT), the cyber system and physical system are highly connected and, therefore, the threat of cyberattacks on the power grid also increases. Intruders seeking to cause damages to the grid can compromise the communication systems to launch an attack on the power grid.

In December 2015, the power grid in Ukraine experienced a cyberattack by hackers (Ahern, 2017; Liang *et al.*, 2017). The damage caused by the sophisticated attack was a power outage affecting about 225,000 customers for about 6 h. The hacker implemented malware using a phishing email to obtain the VPN credential. From this attack, the hacker launched remote control actions through the control center computers. Denial of Service (DoS) attacks jammed phone reports of the outage to the call center. Furthermore, the data destruction software, KillDisk, was used to erase the reboot software in the workstation, causing a delay in power system restoration. Further observations can be made concerning the Ukraine attack scenario: (1) First, the hackers were knowledgeable about the operation of the targeted grid, (2) the hackers were able to manipulate the cyber–power system (CPS) from the Distribution System Operator (DSO) control center, and (3) the hackers had knowledge of critical control and operation devices. The in-depth information was obtained by penetrating the Supervisory Control And Data Acquisition (SCADA) system and staying undetected for at least 6 months. After observing for 6 months, the hackers gained sufficient knowledge about the operation and critical information of the power system. With the information garnered, the hacker(s) conducted an attack through the SCADA system to operate circuit breakers in the substations, causing a power outage.

As demonstrated by the real-world cyberattack, it is critical to fully understand the vulnerabilities of the CPS to develop the capabilities for detecting cyber intrusions and take timely mitigation actions. Although cyber intrusions can be launched by compromising control center computers, damages could also be caused by man-in-the-middle attacks on the communication system between the control center and field devices. Therefore, the defense of the communication system is a critical issue for power systems.

Cyber security issues arise when power system components are provided with remote monitoring and control capabilities over public communication infrastructures. Remote monitoring and control for power grids have been the industry practice. This would not be a problem if the utility communication networks are private and isolated from the Internet. The problem is that the utility private communication networks, Operational Technology (OT) systems, for substation and control center communications may be connected with the general Information Technology (IT) systems used for other purposes (Nazir *et al.*, 2017) such as electricity trading, and these IT systems are in turn connected to the Internet. While there are firewalls between IT and OT systems, the firewalls may have vulnerabilities. Furthermore, some distribution system operators use public communication networks for their distribution networks (Nazir *et al.*, 2017) such as 3G/4G/5G for the pole-mounted devices. They also communicate with the control centers.

Development of the Smart Grid in recent years by large-scale deployment of ICT leads to fast-increasing connectivity of devices and systems in the power grid. Smart grid development in the United States is primarily concerned with Phasor Measurement Units (PMUs) for the transmission system as well as remote control switches and voltage/var control devices in the distribution systems. The remote monitoring and control capabilities are also created for millions of smart meters at the customer locations and DERs, including renewable energy, energy storage, and responsive load. Indeed, Advanced Metering Infrastructure (AMI) has been installed for communication and control between the utility company and numerous smart meters. As a result of the DERs, the architecture of the power grid is rapidly evolving from a centralized utility service to a distributed or decentralized structure (Liu *et al.*, 2016b). For example, Hawaii reached 23% of renewable electricity while California has 26% renewable (Sgouras *et al.*, 2017; Finster and Baumgart, 2015) and targets a 50% level by 2030. Deployment of DERs is often conducted by nonutility parties and, therefore, the utility system may not have full control of the devices. AMI also brings new communication and control features through smart meters. As a result, additional risks emerge due to a large number of devices and noncontrollable access points (Liu *et al.*, 2016a; INL, 2007; INL, 2008; Rohde, 2005).

This survey paper is intended to serve as a module in senior-level undergraduate as well as graduate courses in power engineering. The objective of this paper, therefore, is to provide fundamental concepts of cyber security for the distribution system as a CPS. To meet the objective, vulnerabilities of cyber intrusions and mitigation strategies are discussed. The remaining sections are organized as follows. The evolution of the ICT for the power grid, sources of vulnerabilities, and cyber security measures are presented in Section 2. Sections 3 and 4 describe the ICT in the power system environment. Section 5 focuses on the cybersecurity issues of a distribution system, while Section 6 discusses smart grid communication standards and protocols. In Section 7 detection of cyber intrusions in distribution systems is considered. Mitigation strategies are provided in Section 8. Simulation cases based on the CPS model are presented in Section 9, and the paper is concluded in Section 10.

References

Ahern, M. F. (2017). "Cybersecurity in power systems". *IEEE Potentials*. 36(5): 8–12.

Al-Shaer, E. S. and H. H. Hamed (2004). "Discovery of policy anomalies in distributed firewalls". *IEEE INFOCOM*. 4: 2605–2616.

Amanullah, M. T. O., A. Kalam, and A. Zayegh (2005). "Network security vulnerabilities in SCADA and EMS". In: *IEEE/PES Transmission & Distribution Conference & Exposition: Asia and Pacific*. Dalian. 1–6.

Amoah, A., S. Camtepe, and E. Foo (2016). "Securing DNP3 broadcast communications in SCADA systems". *IEEE Transactions on Industrial Informatics*. 12(4): 1474–1485.

Appiah-Kubi, J. and C. C. Liu (2020). "Decentralized intrusion prevention (DIP) against Co-ordinated cyberattacks on distribution automation systems". *IEEE Open Access Journal of Power and Energy*. 7: 389–402.

Bakken, D. E., A. Bose, C. H. Hauser, D. E. Whitehead, and G. C. Zweigle (2011). "Smart generation and transmission with coherent, real-time data". *Proceedings of the IEEE*. 99(6): 928–951.

Barai, G. R., S. Krishnan, and B. Venkatesh (2015). "Smart metering and functionalities of smart meters in smart grid — A review". *IEEE Electrical Power and Energy Conference (sEPEC)*: 138–145.

Barbosa, R. R. R., R. Sadre, and A. Pras (2013). “Flow whitelisting in SCADA Networks”. *International Journal of Critical Infrastructure Protection*. 6: 150–158.

Berthier, R. and W. Sanders (2011). “Specification-based intrusion detection for advanced metering infrastructures”. In: *Proc. IEEE 17th Pacific Rim Int. Symp. Dependable Computing*. 184–193.

CENTRON (2006). *CENTRON Meter Technical Reference Guide*. Available online at: http://www.smartmetereducationnetwork.com/uploads/how-to-tell-if-I-have-a-ami-dte-smart-advanced-meter/Itron%20Centron%20Meter%20Technical%20Guide1482163-201106090057150.pdf. Liberty Lake, WA: Itron Inc.

Chapman, D., A. Fox, and R. Stiffler (2001). *Cisco Secure PIX Firewalls*. Cisco Press.

Chen, Y., J. Hong, and C. C. Liu (2018). “Modeling of intrusion and defense for assessment of cyber security at power substations”. *IEEE Transactions on Smart Grid*. 9(4): 2541–2552.

Cheng, X., W. J. Lee, and X. Pan (2017). “Modernizing substation automation systems: Adopting IEC standard 61850 for modeling and communication”. *IEEE Industry Applications Magazine*. 23(1): 42–49.

Choi, I.-S., J. Hong, and T.-W. Kim (2020). “Multi-agent based cyber attack detection and mitigation for distribution automation system”. *IEEE Access*. 8: 183495–183504.

Clavel, F., E. Savary, P. Angays, and A. Vieux-Melchior (2015). “Integration of a new standard: A network simulator of IEC 61850 architectures for electrical substations”. *IEEE Industry Applications Magazine*. 21(1): 41–48.

CPUC (2015). “Recommendations for Utility Communications with Distributed Energy Resources (DER) Systems with Smart Inverters”. Sacramento, CA: California Energy Commission and California Public Utilities Commission (SIWG Phase 2). Available online at: https://www.energy.ca.gov/electricity_analysis/rule21/documents/SIWG_Phase_2_Communications_Recommendations_for_CPUC.pdf.

CSIP (2018). "IEEE 2030.5 Implementation Guide for Smart Inverters". San Jose, CA: Common Smart Inverter Profile Working Group., SunSpec 2018. Available online at: https://sunspec.org/wp-content/uploads/2018/03/CSIPImplementationGuidev2.003-022018-1.pdf.

Ericsson, G. (2007). "Toward a framework for managing information security for an electric power utility—CIGRÉ experiences". *IEEE Transactions on Power Delivery*. 22(3): 1461–1469.

Esmalifalak, M., L. Liu, N. Nguyen, R. Zheng, and Z. Han (2017). "Detecting stealthy false data injection using machine learning in smart grid". *IEEE Systems Journal*. 11(3): 1644–1652.

Falliere, N., L. O. Murchu, and E. Chien (2011). "W32.Stuxnet dossier". *Symantec Security Response, Version 1.4*. Available online at: https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

Fan, Y., Z. Zhang, M. Trinkle, A. D. Dimitrovski, J. B. Song, and H. Li (2015). "A cross-layer defense mechanism against GPS spoofing attacks on PMUs in smart grids". *IEEE Transactions on Smart Grid*. 6(6): 2659–2668.

Farraj, A., E. Hammad, A. A. Daoud, and D. Kundur (2016). "A game-theoretic analysis of cyber switching attacks and mitigation in smart grid systems". *IEEE Transactions on Smart Grid*. 7(4): 1846–1855.

Fawaz, A., R. Berthier, and W. H. Sanders (2012). "Cost modeling of response actions for automated response and recovery in AMI". *2012 IEEE Third International Conference on Smart Grid Communications (SmartGridComm)*: 348–353.

Finster, S. and I. Baumgart (2015). "Privacy-aware smart metering: A survey". *IEEE Communications Surveys & Tutorials*. 17(2): 1088–1101.

Fischer, R., N. Schulz, and G. H. Anderson (2000). "Information management for an automated meter reading system". In: *Proceedings of the 62nd American Power Conference*.

Gilchrist, G. (2008). "Secure authentication for DNP3". In: *Proc. IEEE Power Energy Soc. Gen. Meeting-Convers. Del. Elect. Energy 21st Century*. Pittsburgh, PA, USA. 1–3.

Hahn, A. and M. Govindarasu (2013). "Model-based intrusion detection for the smart grid (MINDS)". In: *ACM Proc. of the Eighth Annual CSIIRW*. New York, NY, USA.

Hamed, H., E. Al-Shaer, and W. Marrero (2005). "Modeling and verification of IPSec and VPN security policies". In: *13th IEEE International Conference on Network Protocols (ICNP'05)*. 10.

Hari, A., S. Suri, and G. Parulkar (2000). "Detecting and resolving packet filter conflicts". In: *Proceedings of the IEEE INFOCOM 2000. Conference on Computer Communications*. 1203–1212.

Hayes, G. and K. El-Khatib (2013). "Securing modbus transactions using hash-based message authentication codes and stream transmission control protocol". In: *2013 Third Intl. Conf. Commun. and Inf. Technol. (ICCIT)*. Beirut. 179–184.

He, D., S. Chan, and M. Guizani (2017). "Cyber security analysis and protection of wireless sensor networks for smart grid monitoring". *IEEE Wireless Communications*. 24(6): 98–103.

Hong, J., C. C. Liu, and M. Govindarasu (2014). "Integrated anomaly detection for cyber security of the substations". *IEEE Transactions on Smart Grid*. 5(4): 1643–1653.

Huseinović, A., S. Mrdović, K. Bicakci, and S. Uludag (2020). "A Survey Of Denial-Of-service attacks and solutions in the smart grid". *IEEE Access*. 8: 177447–177470.

Hussain, S. M. S., T. S. Ustun, and A. Kalam (2020). "A review of IEC 62351 security mechanisms for IEC 61850 message exchanges". *IEEE Transactions on Industrial Informatics*. 16(9): 5643–5654.

IEEE (2012). "Intruders in the grid". *IEEE Power & Energy Magazine*. Available online at: https://magazine.ieee-pes.org/january-february-2012/intruders-in-the-grid/.

IEEE (2016). *IEEE Standard for Low-Rate Wireless Networks, IEEE Standard 802.15.4-2015*. (Revision of IEEE Standard 802.15.4-2011).

IEEE 2030.5-2018 (2018). "IEEE standard for smart energy profile application protocol".

INL (2007). *National SCADA Test Bed: Fact Sheet*. Idaho National Laboratory (INL).

INL (2008). *Common Cyber Security Vulnerabilities Observed in Control System Assessments by the INL NSTB Program*. Idaho National Laboratory (INL).

Jiang, Y., C. C. Liu, M. Diedesch, E. Lee, and A. K. Srivastava (2016). "Outage management of distribution systems incorporating information from smart meters". *IEEE Transactions on Power Systems*. 31(5): 4144–4154.

Karimipour, H., A. Dehghantanha, R. M. Parizi, K. R. Choo, and H. Leung (2019). "A deep and scalable unsupervised machine learning system for cyber-attack detection in large-scale smart grids". *IEEE Access*. 7: 80778–80788.

Khalifa, T., K. Naik, and A. Nayak (2011). "A survey of communication protocols for automatic meter reading applications". *IEEE Communication on Surveys & Tutorials*. 13(2): 168–182.

Khanna, K., B. K. Panigrahi, and A. Joshi (2018). "AI-based approach to identify compromised meters in data integrity attacks on smart grid". *IET Generation, Transmission, and Distribution*. 12(5): 1052–1066.

Krebs, B. (2012). *FBI: Smart Meter Hacks Likely to Spread*. Available online at: http://krebsonsecurity.com/2012/04/fbi-smart-meterhacks-likely-to-spread/.

Kushner, D. (2013). "The real story of Stuxnet". *IEEE Spectrum*. 50(3): 48–53.

Li, G. W., W. Y. Ju, and D. Y. Shi (2012). "Functional vulnerability assessment of SCADA network". In: *2012 Asia-Pacific Power and Energy Engineering Conference*. Shanghai. 1–4.

Liang, G., S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong (2017). "The 2015 Ukraine blackout: Implications for false data injection attacks". *IEEE Transactions on Power Systems*. 32(4): 3317–3318.

Liang, X., X. Li, R. Lu, X. Lin, and X. Shen (2013). "UDP: Usage-based dynamic pricing with privacy preservation for smart grid". *IEEE Transactions on Smart Grid*. 4(1): 141–150.

Liu, J., Y. Xiao, S. Li, W. Liang, and C. L. P. Chen (2012). "Cyber security and privacy issues in smart grids". *IEEE Communications Surveys & Tutorials*. 14(4): 981–997. Fourth Quarter 2012.

Liu, X., P. Zhu, Y. Zhang, and K. Chen (2015). "A collaborative intrusion detection mechanism against false data injection attack in advanced metering infrastructure". *IEEE Transactions on Smart Grid*. 6(5): 2435–2443.

Liu, Y., S. Hu, and T. Ho (2014). "Vulnerability assessment and defense technology for smart home cybersecurity considering pricing cyberattacks". In: *2014 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*. San Jose, CA. 183–190.

Liu, Y., S. Hu, and T. Ho (2016a). "Leveraging strategic detection techniques for smart home pricing cyberattacks". *IEEE Transactions on Dependable and Secure Computing*. 13(2): 220–235.

Liu, Y., S. Hu, and A. Y. Zomaya (2016b). "The hierarchical smart home cyberattack detection considering power overloading and frequency disturbance". *IEEE Transactions on Industrial Informatics*. 12(5): 1973–1983.

McLaughlin, S., B. Holbert, A. Fawaz, R. Berthier, and S. Zonouz (2013). "A multi-sensor energy theft detection framework for advanced metering infrastructures". *IEEE Journal on Selected Areas in Communications*. 31(7): 1319–1330.

McLaughlin, S., D. Podkuiko, and P. McDaniel (2009). "Energy Theft in the Advanced Metering Infrastructure". In: *4th Workshop on Critical Information Infrastructures Security*. 176–187.

Mitchell, R. and I. R. Chen (2013). "Behavior-rule based intrusion detection systems for safety critical smart grid applications". *IEEE Transactions on Smart Grid*. 4(3): 1254–1263.

Mo, Y., R. Chabukswar, and B. Sinopoli (2014). "Detecting integrity attacks on SCADA systems". *IEEE Transactions on Control Systems and Technology*. 22(4): 1396–1407.

Modbus (2006). *Modbus Application Protocol Specification, V1.1B*. Modbus Organization. Available online at: http://www.modbus-IDA.org.

Moya, C. and J. Wang (2018). "Developing correlation indices to identify coordinated cyber-attacks on power grids". *IET Cyber-Physical Systems: Theory & Applications*. 3(4): 178–186.

Namboodiri, V., V. Aravinthan, S. N. Mohapatra, B. Karimi, and W. Jewell (2014). "Toward a secure wireless-based home area network for metering in smart grids". *IEEE Systems Journal*. 8(2): 509–520.

Nazir, S., S. Patel, and D. Patel (2017). "Assessing and augmenting SCADA cyber security — A survey of techniques". *Computers & Security*. 70: 436–454.

NCCIC and ICS-CERT (2016). "NCCIC/ICS-CERT 2015 Year in Review". 2016. Available online at: https://ics-cert.uscert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2015_Final_S508C.pdf.

NERC (2006). "North American Electric Reliability Corporation". CIP Standard. Available online at: http://www.nerc.com/fileUploads/File/Standards/Revised_Implementation_Plan_CIP-002-009.pdf (accessed on 2 May 2006).

NIST (2010). *Guidelines for Smart Grid Cyber Security, NISTIR 7628*. National Institute for Standards and Technology. Available online at: http://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf (accessed on 30 September 2010).

NIST (2014). *The Cyber Security Coordination Task Group: Smart Grid Cyber Security Strategy and Requirements*. [Online]. National Institute for Standards and Technology. Available online at: http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol2.pdf (accessed on 2 October 2014).

Padilla, E., K. Agbossou, and A. Cardenas (2014). "Towards smart integration of distributed energy resources using distributed network protocol over ethernet". *IEEE Transactions on Smart Grid*. 5(4): 1686–1695.

Phan, R. C. W. (2012). "Authenticated modbus protocol for critical infrastructure protection". *IEEE Transactions on Power Delivery*. 27(3): 1687–1689.

PNNL (n.d.). "The U.S. Pacific Northwest National Laboratory (PNNL)". AMI communication requirements to implement demand-response: Applicability of hybrid spread spectrum wireless". Available online at: http://www.pnnl.gov/main/publications/external/technical_reports/PNNL-20806.pdf.

Premaratne, U. K., J. Samarabandu, T. S. Sidhu, R. Beresh, and J. C. Tan (2010). "An intrusion detection system for IEC61850 automated substations". *IEEE Transactions on Power Delivery*. 25(4): 2376–2383.

Qi, J., A. Hahn, X. Lu, J. Wang, and C. C. Liu (2016). "Cybersecurity for distributed energy resources and smart inverters". *IET Cyber-Physical Systems: Theory & Applications*. 1(1): 28–39.

Rashed Mohassel, R., A. Fung, F. Mohammadi, and K. Raahemifar (2014). "A survey on advanced metering infrastructure". *International Journal of Electrical Power & Energy Systems*: 63.

Rohde, M.-R.-P. (2005). *Cyber Assessment Methods for SCADA Security*. Instrumentation, Syst. Autom. Soc. (ISA), Tech.

Rosenbaum, H. (2012). *Danville Utilities Sees Increase in Meter Tampering*. Available online at: http://www.wset.com/story/20442252/danville-utilities-sees-increase-inmeter-tampering.

SANS and Electricity Information Sharing and Analysis Center (E-ISAC) (2016). "Analysis of the cyber attack on the ukrainian power grid". March 18. Available online at: http://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf.

Sapegin, A., A. Amirkhanyan, M. Gawron, F. F. Cheng, and C. Meinel (2015). "Poisson-based anomaly detection for identifying malicious user behaviour". In: Mobile, Secure, and Programmable Networking, MSPN 2015, *Lecture Notes in Computer Science*. Vol 9395. Springer.

SEIA (2018). "Solar Energy Industries Association". "Solar State by State," SEIA: Washington, DC. Available online at: https://www.seia.org/states-map.

SGIP (2014). "Smart Grid Interoperability Panel (SGIP)". Distributed Energy Resources (DER): Hierarchical Classification of Use Cases and the Process for Developing Information Exchange Requirements and Object Models," White Paper, 2014. Available online at: http://www.sgip.org/wp-content/uploads/Distributed-Energy-Resources_DER-Hierarchical-Classification-of-Use-Cases-and-the-Process-for-Developing-Information-Exchange-Requirements-and-Object-Models-2014-07-18.pdf.

Sgouras, K. I., A. N. Kyriakidis, and D. P. Labridis (2017). "Short-term risk assessment of Botnet attacks on advanced metering infrastructure". *IET Cyber-Physical Systems: Theory & Applications*. 2(3): 143–151.

Shahzad, A., S. Musa, A. Aborujilah, and M. Irfan (2014). "Industrial control systems (ICSs) vulnerabilities analysis and SCADA security enhancement using testbed encryption". In: *Proceedings of the 8th International Conference on Ubiquitous Information Management and Communication. (ICUIMC'14)*. New York, NY. 7.

Smith, R. (2014). "Assault on California power station raises alarm on potential for terrorism". *The Wall Street Journal*. Available online at: http://online.wsj.com/news/articles/SB10001424052702304851104579359141941621778.

Song, K. Y., K. S. Yu, and D. Lim (2015). "Secure frame format for avoiding replay Attack in distributed network protocol (DNP3)". In: *International Conference on Information and Communication Technology Convergence (ICTC)*. Jeju. 344–349.

Spolar, S. (2012). *Cyber Attack Task Force*. Atlanta, GA: North American Electric Reliability Corporation. Final Rep.

Sridhar, S., M. Govindarasu, and C. C. Liu (2012). *Control and Optimization Methods for Electric Smart Grids*. vol. 3. Springer, 275–294.

Srikantha, P. and D. Kundur (2016). "A DER attack-mitigation differential game for smart grid security analysis". *IEEE Transactions on Smart Grid*. 7(3): 1476–1485.

Stefanov, A., C. C. Liu, and K. Liyanage (2015). "ICT modeling for cosimulation of integrated cyber–power systems". *Securing Cyber-Physical Systems*. CRC Press, pp. 46–81.

Stouffer, K., J. Falco, and K. Scarfone (2011). *Guide to Industrial Control Systems (ICS) Security*. Washington, DC: Nat. Inst. Standards Technol. (NIST), U.S. Dept. Commerce (Special Pub. 800-82).

Strobel, M., N. Wiedermann, and C. Eckert (2016). "Novel weaknesses in IEC 62351 protected smart grid control systems". In: *IEEE International Conference on Smart Grid Commun. (SmartGridComm)*. Sydney, NSW. 266–270.

Sun, C. C., A. Hahn, and C. C. Liu (2018). "Cyber security of a power grid: State-of-the-art". *International Journal of Electrical Power & Energy Systems*. 99: 45–56.

Sun, Q., H. Li, Z. Ma, C. Wang, J. Campillo, Q. Zhang, F. Wallin, and J. Guo (2016). "A comprehensive review of smart energy meters in intelligent energy networks". *IEEE Internet of Things Journal*. 3(4): 464–479.

Ten, C. W., J. Hong, and C. C. Liu (2011). "Anomaly detection for cybersecurity of the substations". *IEEE Transactions on Smart Grid*. 2(4): 865–873.

Ten, C. W., C. C. Liu, and G. Manimaran (2008). "Vulnerability assessment of cybersecurity for SCADA systems". *IEEE Transactions on Power Systems*. 23(4): 1836–1846.

Ten, C.-W., G. Manimaran, and C. C. Liu (2010). "Cybersecurity for critical infrastructures: Attack and defense modeling". *IEEE Transactions on Systems, Man, and Cybernetics Part A: Systems and Humans*. 40(4): 853–865.

USDoE (2011). "The U.S. Department of Energy, Energy Sector Control Systems Working Group (ESCSWG)". Roadmap to achieve energy delivery system cyber security". Available online at: http://energy.gov/oe/downloads/roadmap-achieve-energy-delivery-systems-cybersecurity-2011.

USDoE (2016). "Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector". The U.S. Department of Energy. Available online at: https://energy.gov/sites/prod/files/2017/01/f34/Cyber%20Threat%20and%20Vulnerability%20Analysis%20of%20the%20U.S.%20Electric%20Sector.pdf.

Wei, F., Z. Wan, and H. He (2020). "Cyber-attack recovery strategy for smart grid based on deep reinforcement learning". *IEEE Transactions on Smart Grid*. 11(3): 2476–2486.

Wu, J., J. Xiong, P. Shil, and Y. Shi (2014). "Real time anomaly detection in wide area monitoring of smart grids". In: *IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*. San Jose, CA. 197–204.

Yang, Y., K. McLaughlin, T. Littler, S. Sezer, B. Pranggono, and H. F. Wang (2013). "Intrusion detection system for IEC 60870-5-104 based SCADA networks". In: *2013 IEEE Power & Energy Society General Meeting*. Vancouver, BC. 1–5.

Yang, Y., H. Q. Xu, L. Gao, Y. B. Yuan, K. McLaughlin, and S. Sezer (2017). "Multidimensional intrusion detection system for IEC 61850-based SCADA networks". *IEEE Transactions on Power Delivery*. 32(2): 1068–1078.

Yuan, L., H. Chen, J. Mai, C. N. Chuah, Z. Su, and P. Mohapatra (2006). "FIREMAN: A toolkit for firewall modeling and analysis". In: *2006 IEEE Symposium on Security and Privacy (S&P'06)*. Berkeley/Oakland, CA.

Zhang, X. and K. K. Parhi (2002). "Implementation approaches for the advanced encryption standard algorithm". *IEEE Circuits and Systems Magazine*. 2(4): 24–46.

Zhang, Y., L. Wang, W. Sun, R. C. Green II, and M. Alam (2011). "Distributed intrusion detection system in a multi-layer network architecture of smart grids". *IEEE Transactions Smart Grid*. 2(4): 796–808.

Zhang, Y., L. Wang, Y. Xiang, and C. W. Ten (2016). "Inclusion of SCADA cyber vulnerability in power system reliability assessment considering optimal resources allocation". *IEEE Transactions on Power Systems*. 31(6): 4379–4394.

Zhang, Y., L. Wang, Y. Xiang, and C.-W. Ten (2015). "Power system reliability evaluation with SCADA cybersecurity considerations". *IEEE Transactions on Smart Grid*. 6(4): 1707–1721.